International Journal of Interdisciplinary Innovative Research & Development (IJIIRD)

ISSN: 2456-236X

Vol. 10 Issue 01 | 2025

ATM AUTOMATED DOORLOCK WITH SMS ALERT AND CALLING USING GSM

Priyanshu Ambekar[1], Tejas Kamble[2], Komal Bahurashi[3], Srusha Gedam[4], Manoj Vairalkar[5]

[1,2,3,4] Student, Computer Science Engineering, Govindrao Wanjari College Of Engineering & Technology Nagpur, Maharashtra, India

[5]Assistant Professor, Computer Science Engineering, Govindrao Wanjari College Of Engineering & Technology Nagpur, Maharashtra, India

DOI: 10.5281/zenodo.15751487

ABSTRACT

This project is designed to strengthen the security and manageability of ATM enclosures. It features an automated door locking system integrated with GSM communication to provide real-time alerts and remote monitoring. Access to the ATM cabin is restricted to authorized users, who can verify their identity using methods such as RFID cards, passwords, or biometric sensors.

If the system detects an unauthorized entry attempt or any irregular behavior, it promptly sends an SMS alert to the responsible authorities and can also initiate a voice call via the GSM module for immediate notification. To support security audits, all access events are recorded and stored in a log for future reference.

The system offers a cost-effective and reliable approach to improving ATM security. By merging automated access control with GSM-based communication, it delivers a modern solution to safeguard ATM infrastructure and enhance user safety.

Keyword: ***- ATM security, Automated door lock, GSM module, SMS alert, Calling system, RFID authentication, Biometric access, Unauthorized access, Real-time notification, Security breach, Access control system, Audit trail, Customer safety, Embedded system, Smart locking system.***

1. INTRODUCTION

Motion-Based Anti-Theft Detection System with SMS Alert and Calling via GSM centers around the development of a practical and low-cost home security system. The author explores the design and operation of modern security systems and demonstrates how these principles can be applied in a budget-friendly and easily maintainable setup. The topic is well-suited for a Bachelor’s thesis, offering a balanced blend of theoretical knowledge and hands-on experience.

The project aimed to create a functional prototype of a home security system that could detect unauthorized access and communicate alerts wirelessly. Key features include a password-protected entry, motion-based intruder detection, an audible alarm, and wireless interaction between the system and the user via GSM technology.

The core of the system is powered by the ATMega16 microcontroller, which manages all operations. The software development and programming were primarily carried out using AVR Studio on a Windows platform. After assembling and testing the components, the system performed successfully. Sensors detected motion as expected, the alarm was triggered appropriately, and the control interface provided a simple and effective way for users to interact with the system.

The enhanced version of this project—**“Motion-Based Anti-Theft Detection System with SMS Alert and Calling Using GSM”**—was developed to protect restricted areas in homes or offices. The system uses embedded technology to notify the owner via SMS when unauthorized movement is detected. By integrating a GSM module, it allows remote control and monitoring through text commands, making it possible for users to manage security even when away.

This type of GSM-based system is especially relevant in today’s world, where mobile devices play a significant role not only in communication but also in security. The proposed solution offers an efficient alternative to employing security personnel, giving homeowners greater peace of mind and autonomy in securing their property. Its applications are broad and adaptable to the growing demands of modern security challenges.

2. LITERATURE REVIEW

This literature review examines the technological foundations and existing research relevant to the development of automated door lock systems enhanced by GSM-based alert mechanisms, particularly within the context of ATM security. The focus is on evaluating how modern technologies—such as RFID, biometrics, and GSM communication—are utilized to enhance security and prevent unauthorized access to ATM enclosures.

Automated door locking mechanisms have become increasingly common in security-sensitive environments. Technologies like RFID authentication, PIN codes, and biometric verification (e.g., fingerprint or facial recognition) are frequently employed to regulate access. For example, a study by Ahmed et al. (2020) evaluated systems that combined fingerprint and PIN-based authentication, demonstrating improved reliability in controlled access environments.

Traditional mechanical locks are often inadequate for ATMs, as they are prone to physical attacks and tampering. With ATMs being a central component of banking infrastructure, ensuring their physical and operational security has become a major concern. Despite the use of standard surveillance and alarm systems, these alone are insufficient to deter increasingly sophisticated security threats. Therefore, automated systems that integrate real-time alert features have become a critical advancement in this field.

Automated door lock systems in ATMs typically use electronic locking mechanisms that activate upon successful authentication through various means, such as magnetic cards, biometric scans, or password entry. Advanced systems may also include environmental sensors that detect unauthorized access attempts or unusual physical interactions with the ATM. When suspicious behavior is detected, the system can automatically lock down and initiate alerts.

One significant enhancement in modern systems is the incorporation of GSM (Global System for Mobile Communication) technology. GSM modules—such as SIM800L or SIM900—facilitate communication via SMS and voice calls. These modules can be integrated into ATM security systems to provide immediate alerts to authorized personnel. When an unauthorized access attempt is detected, the system can automatically send an SMS or place a call to bank security teams, nearby branches, or emergency responders. This feature enables fast response times even in remote locations where internet connectivity may be unreliable.

SMS alerts are particularly useful due to their simplicity and broad network coverage. They offer a reliable way to inform the concerned parties in real-time without depending on Wi-Fi or broadband connections. In more critical scenarios, the GSM module can also initiate a voice call, ensuring that urgent threats are communicated immediately. This redundancy in alert mechanisms strengthens the responsiveness of the overall system.

To further ensure communication security, some systems employ basic encryption methods to prevent interception or manipulation of alert messages. Power reliability is another key factor in the consistent operation of these systems. Backup power sources such as UPS units or solar panels are often integrated to keep the system active during outages. Additionally, energy-efficient GSM modules help extend the system's operational lifespan with minimal maintenance.

However, GSM-based systems also face limitations. One common challenge is the dependency on mobile networks, which may not always be available or strong in certain areas, potentially delaying the alerts. Another concern involves the vulnerability of GSM communications to hacking or unauthorized access, though such risks can be mitigated with appropriate security protocols.

Looking forward, ATM security solutions can benefit from emerging technologies such as the Internet of Things (IoT), artificial intelligence (AI), and blockchain. AI can support advanced threat detection by analyzing behavior patterns and predicting potential risks. IoT sensors could be used to monitor environmental changes (e.g., vibrations, temperature, or pressure changes), offering another layer of threat identification. Blockchain could help secure the transmission of data between ATMs and banking servers, enhancing integrity and reducing the risk of tampering.

In conclusion, the integration of GSM-enabled automated door locking systems offers a practical and efficient solution to ATM security challenges. The combination of access control, real-time communication, and alert capabilities enhances protection for both ATM infrastructure and users. Continued research and technological integration—particularly with AI, IoT, and blockchain—can lead to more intelligent and adaptive security systems capable of addressing modern threats more effectively.

3. RELATED WORK

The integration of GSM communication with ATM security systems has been a key area of research and practical implementation aimed at enhancing protection against unauthorized access. These systems typically incorporate automated door locks, SMS alerts, and call functionalities to ensure that any suspicious activity is promptly detected and reported to responsible authorities.

One foundational development in this area involved GSM-based ATM security solutions using microcontrollers to manage automated locking mechanisms and alert systems. For example, a project presented by Venugopal et al. (2012) introduced a system where a microcontroller operated an electronic lock and interfaced with a GSM module to send real-time SMS notifications during security breaches. The system was capable of identifying unauthorized access attempts or abnormal user behavior and would automatically send a warning message to pre-assigned phone numbers, such as those of bank officials or security personnel. In addition to SMS, the system had the capacity to place phone calls for urgent notification, laying a significant groundwork for future GSM-integrated ATM security systems.

Another notable contribution was made by Subashini and Gnanasekaran (2015), who developed an ATM protection system that integrated a GSM module, sensors, and a microcontroller to enhance ATM security, particularly during non-operational hours. This setup used sensors to detect physical tampering or access attempts. Upon detecting suspicious activity, the microcontroller activated the lock and prompted the GSM module to send an alert via SMS to designated bank personnel. In critical scenarios, it could also initiate a phone call to enable faster responses. This study emphasized the role of automation and real-time communication in reducing the response time during potential security threats.

These examples reflect broader trends in ATM security research, where combining microcontroller-based automation with GSM technology has improved both the physical security and communication responsiveness of ATMs. Projects in this domain often incorporate other features such as motion detection, password entry systems, and in some cases, biometric access control, to ensure multi-level authentication before granting access.

The evolution of GSM-based systems has also influenced how modern ATMs are protected. The dual capability of SMS and calling allows for layered communication in emergency situations, reducing dependence on a single alert method. Moreover, these systems are particularly effective in remote or low-connectivity areas, where traditional internet-based monitoring solutions might not function reliably.

Despite these advancements, GSM-based systems are not without limitations. Issues such as network signal availability, potential interception of messages, and hardware failure must be addressed for these systems to operate reliably under all conditions. Additionally, future enhancements in ATM security are likely to involve the integration of emerging technologies such as artificial intelligence for behavioral analysis, blockchain for secure and transparent communication, and IoT devices for broader environmental monitoring.

In summary, the implementation of GSM-based ATM door locking systems with real-time SMS and call alerts has demonstrated significant potential in improving ATM security. As technology continues to evolve, future research and development will likely focus on enhancing these systems with more secure, intelligent, and resilient components, ensuring that ATMs remain protected against both physical and digital threats.

4. PROPOSED WORK

This project proposes the design and development of an advanced ATM security solution that incorporates automated locking, real-time alerts, and communication functionalities using GSM technology. The primary aim is to strengthen ATM protection against threats such as unauthorized entry, tampering, and theft. The system is designed to automatically secure the ATM by locking its door upon detecting suspicious activity and to immediately notify bank personnel or law enforcement via SMS and phone calls.

This solution is developed to overcome several critical weaknesses in conventional ATM security mechanisms. By integrating GSM communication with smart sensors and actuators, the system ensures timely alerts and autonomous physical responses, thereby minimizing the potential for unauthorized access or physical damage to the machine.

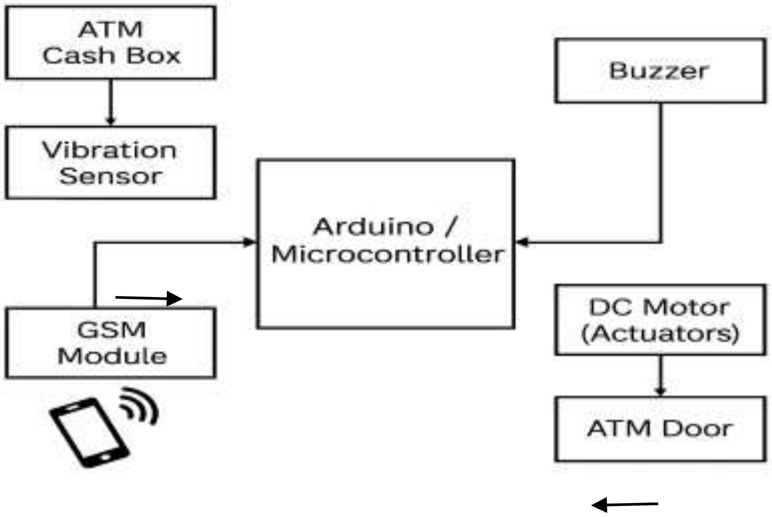

Fig.1. System Architecture Overview

The security system is structured around a layered defense model, consisting of sensors, actuators, communication modules, and a central microcontroller. The main components of the prototype include:

- **Arduino Uno**: A microcontroller development board based on the ATmega328P, serving as the central control unit.
- **Vibration Sensor**: Detects tampering attempts by sensing vibrations, particularly from the cash compartment.
- **DC Motor**: Acts as an actuator to automatically close the ATM door during a security breach.
- **GSM Module**: Sends SMS alerts to predefined phone numbers when suspicious activity is detected.
- **Buzzer**: Generates an audible alarm to deter intruders and alert nearby individuals.

4.1. Operation and Workflow:

The system operates by monitoring vibration levels through the connected sensor. If the detected vibration exceeds a predefined threshold (e.g., 15,000 Hz), the Arduino controller initiates a series of actions:

1. **Audible Alert**: The buzzer is activated to provide immediate local warning.
2. **Door Lock Activation**: The DC motor engages to shut the ATM door, securing the machine from further tampering.
3. **SMS Notification**: Using the GSM module, an alert message—along with the Calling function—is sent to a registered mobile number associated with bank officials or security personnel.

This multi-tiered response system ensures rapid physical protection and immediate remote awareness in the event of a breach.

4.2. System Development and Integration:

The prototype utilizes the Arduino IDE for development, with the sketch (firmware) written in Arduino C. The development board interfaces with a computer via USB for programming and testing. The GPIO (General Purpose Input/Output) pins on the Arduino are used to connect and control analog and digital components such as sensors, motors, and modules.

Each connected device is configured either as input or output, and the controller continuously monitors sensor feedback to trigger necessary actions. The GSM modules work together to construct and deliver detailed alerts, including both the nature of the incidents.

5. CONCLUSION

The design and deployment of an ATM automated door locking system integrated with GSM-based SMS and calling capabilities offer a strong and practical approach to mitigating key security challenges faced by modern Automated Teller Machines (ATMs). As the number of ATM installations continues to rise globally, the need to prevent unauthorized access, tampering, and theft has become more critical than ever.

This system addresses these concerns by incorporating an intelligent electronic locking mechanism, supported by real-time alerts and communication through GSM technology. In the event of suspicious activity or attempted breaches, the system can instantly notify designated security personnel or authorities via SMS and phone calls, enabling swift intervention and minimizing damage or theft.

The proposed solution stands out for its reliability, cost-effectiveness, and ease of implementation. It not only reinforces physical security at the ATM site but also enables remote monitoring and rapid response through automated, wireless communication.

Looking ahead, the system holds the potential for further enhancement by integrating emerging technologies such as encrypted communication, AI-based threat detection, and predictive maintenance. These advancements will strengthen ATM security systems, making them more adaptive and resilient in the face of evolving threats in an increasingly connected environment.

6. ACKNOWLEDGEMENT

I wish to express my deep sense of gratitude to Govindrao Wanjari College of Engineering and Technology, Nagpur, for providing me with the opportunity to fulfill my most cherished goal. My heartfelt thanks to our Principal, Dr. S. A. Chavan, for the invaluable support and encouragement extended to me throughout the completion of my project.

I extend my immense gratitude to the Head of the Department, Prof. Vivekanand P. Thakare, for his continuous motivation, inspiration, and unwavering support, which played a pivotal role in the successful completion of my project.

I would like to take this opportunity to express my sincere thanks to project guide, Prof. Manoj Vairalkar. His energy, creativity, and exceptional coding skills have been a constant source of motivation and have significantly contributed to the successful completion of my project.

A special acknowledgment goes to our Project Incharge, Prof. Nitin Thakre, from the Department of Computer Science & Engineering. His continuous support, motivation, enthusiasm, and guidance, along with constructive criticism, played a crucial role in bringing this project to fruition.

Lastly, but certainly not the least, I express my heartfelt gratitude to my parents, relatives, friends, and all those whose support, encouragement, and unseen contributions were integral to the realization of this dissertation.

7. REFERENCES

1. Moneycontrol. (2018, August). *Indian banks lost Rs 109.75 crore to theft and online fraud in FY18*. https://www.moneycontrol.com/news/trends/current-affairs-trends/indian-banks-lost-rs-109-75-crore-to-theft-and-online-fraud-in-fy18-2881431.html
2. Kathuria, A., Arora, A., & Singh, M. (2015). A novel approach for microcontroller-based quality assessment system. *2015 International Conference on Soft Computing Techniques and Implementations (ICSCTI)*, IEEE. https://doi.org/10.1109/ICSCTI.2015.7489592
3. Nasution, T. H., Aryza, S., & Harahap, M. E. (2017). Electrical appliances control prototype by using GSM module and Arduino. *4th International Conference on Industrial Engineering and Applications (ICIEA)*, IEEE. https://doi.org/10.1109/IEA.2017.7939237
4. Shriram, S., Ramesh, N., & Raja, K. (2016). Smart ATM surveillance system. *International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, IEEE. https://doi.org/10.1109/ICCPCT.2016.7530322
5. Raj, M. M. E., & Julian, A. (2015). Design and implementation of anti-theft ATM machine using embedded systems. *International Conference on Circuits, Power and Computing Technologies (ICCPCT)*, IEEE. https://doi.org/10.1109/ICCPCT.2015.7159316
6. Küçükbay, S. E., Sert, M., & Yazici, A. (2017). Use of acoustic and vibration sensor data to detect objects in surveillance wireless sensor networks. *21st International Conference on Control Systems and Computer Science (CSCS)*, IEEE. https://doi.org/10.1109/CSCS.2017.35
7. Jacintha, V., Vishnuvardhan, M., & Kaviya, V. (2017). An IoT based ATM surveillance system. *IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*. https://doi.org/10.1109/ICCIC.2017.8524485
8. Umbarkar, S., Gaikwad, A., & Patil, S. (2016). Keypad/Bluetooth/GSM based digital door lock security system. *International Conference on Communication and Signal Processing (ICCASP)*, Atlantis Press. https://doi.org/10.2991/iccasp-16.2017.102
9. Saritha Devi, N., Raju, K. S. R., Madhu, A., & Raja Sekhar, R. (2018). Safety and security for school children’s vehicles using GPS and IoT technology. *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE)*, *7*(6), 97–100. https://doi.org/10.30534/ijatcse/2018/03762018

10. Rao, S. V. R. K., Saritha Devi, M., Kishore, A. R., & Kumar, P. (2018). Wireless sensor network-based industrial automation using Internet of Things (IoT). *International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE)*, *7*(6), 89–92. https://doi.org/10.30534/ijatcse/2018/01762018